TOMÁS AUÑÓN HERNÁNDEZ

Madrid, España | tomasaunon@gmail.com | 676 754 874 |
https://www.linkedin.com/in/tomas-aunon

PERFIL PROFESIONAL

Especialista en **ciberseguridad y administración de sistemas**, con experiencia en entornos **SOC** y formación práctica en **pentesting, gestión de vulnerabilidades y seguridad en redes**.

He desarrollado proyectos de **auditoría web, laboratorios de explotación y CTFs**, aplicando metodologías ofensivas y defensivas en entornos simulados y reales.

Cuento con una sólida base técnica **en redes, sistemas y cloud**, reforzada con práctica continua **en laboratorios de Keepcoding, TryHackMe y HackTheBox**. Actualmente me preparo para la certificación **eJPTv2**, con el objetivo de consolidar mi carrera como **pentester junior / analista de seguridad**.

EXPERIENCIA PROFESIONAL

Colaborador en Proyectos de Ciberseguridad

Keepcoding · Madrid | Mayo 2024 – Marzo 2025

- **Reconocimiento y OSINT:** fingerprinting y enumeración DNS con **Shodan, VirusTotal, Dig y DnsRecon**.
- **Escaneo y vulnerabilidades:** detección de servicios y fallos con **Nmap, Nessus y Greenbone**.
- **Auditorías web:** pruebas con **Burp Suite, Caído, SQLMap, Dirbuster, Dirb y Wfuzz** para identificar vulnerabilidades **OWASP Top 10**.
- **Explotación y post-explotación:** validación de exploits con **Metasploit, Searchsploit/Exploit-DB**, escalada y persistencia en entornos simulados.
- **Defensa y monitorización:** análisis de eventos y respuesta a incidentes con **Splunk, Wazuh, Suricata y honeypots**.
- **Forense y criptografía:** extracción de artefactos en Windows con **KAPE** y prácticas de gestión segura de claves.
- **Sistemas de trabajo: Kali Linux, Tsurugi y Whonix**.

Coordinador de Centro Asistencia Técnica (SOC)

Securitas Seguridad España · Madrid | Nov 2022 – Actualidad

- Coordinación de equipo técnico en **SOC nacional** (soporte remoto de sistemas críticos (alarmas, CCTV, analítica de vídeo, IoT).
- **Monitorización y diagnóstico** de incidencias en redes y dispositivos; priorización y escalado, garantizando continuidad de servicio 24/7.
- Implementación de mejoras que elevaron la **resolución remota** del **18% al 36%.**
- **Estandarización de procedimientos** y guías internas para optimizar tiempos de respuesta.

Supervisor SOC / Revisor de Sistemas / Técnico Especialista

Securitas Seguridad España · Madrid | Abr 2019 – Nov 2022

- Supervisión del Centro de Asistencia Técnica **(SOC)**, priorizando incidencias críticas y garantizando la continuidad de servicio.
- Configuración remota y mantenimiento de sistema (Pacom, Galaxy, SPC, Videofied) y gestión de redes IP.
- Desarrollo de **automatizaciones internas** para reducir tiempos de diagnóstico.
- Elaboración de informes técnicos y coordinación con equipos multidisciplinares y clientes.

Encargado de Transporte Nacional

Cartapaquete S.L. | Oct 2016 – Abr 2018

- Coordinación de envíos nacionales, resolución de incidencias y reporting de calidad y satisfacción.

PROYECTOS DESTACADOS

- **Pentesting Web – Proyecto Final KeepCoding (2025):** Auditoría completa de una aplicación real, explotación de **OWASP Top 10** y elaboración de informe profesional (evaluación 9/10).
- **CTFs y Labs (2024–2025):** Resolución de máquinas en **TryHackMe / HackTheBox / VulnHub** centradas en enumeración, explotación y **priv-esc** (Linux/Windows).

CERTIFICACIONES Y FORMACIÓN COMPLEMENTARIA

- **eJPTv2** – eLearnSecurity Junior Penetration Tester *(en preparación — sep 2025)*
- **TryHackMe** — Jr. Penetration Tester Path *(previsto 2025)*
- **TryHackMe** — Red Team Fundamentals *(previsto 2025)*
- **HackTheBox** — Starting Point & Tier 0/1 *(previsto 2025)*

FORMACIÓN

- **Formación Especializada en Ciberseguridad** | KeepCoding · Madrid | May 2024 – Mar 2025
- **C.F.G.S. Administración de Sistemas Informáticos en Red (ASIR)** | IES CIFP Ignacio Ellacuría · Alcorcón | En curso (finalización prevista 2026)
- **CCNA – Cisco Certified Network Associate** | Salesianos Santo Domingo Salvio · Madrid | 2013 (certif. no vigente)

HABILIDADES TÉCNICAS

- Escaneo de vulnerabilidades (**Nmap, Nessus, Greenbone**) · Auditoría web (**Burp Suite, SQLMap, Gobuster, Dirb, Wfuzz, Nikto, Acunetix, WebGoat**) · Explotación (**Metasploit, Searchsploit, Exploit-DB, Hydra, Hashcat, JohnTheRipper**) · Red Team · Respuesta a incidentes · Hardening de sistemas
- **Monitorización y Detección:** Plataformas SIEM y EDR (**Splunk, Wazuh**) · IDS/IPS (**Suricata**) · Honeypots
- **Sistemas y Redes:** Protocolos TCP/IP · DNS · DHCP · VLANs · Windows Server · Active Directory · Linux · VMware · Hyper-V.
- **Forense y Análisis: KAPE** · Análisis de IOCs · Criptografía aplicada
- **Cloud y DevOps:** AWS, Azure, Docker, CI/CD**.**
- **Lenguajes y Scripting:** Python, Bash, PowerShell, SQL, C#**.**
- **Bases de Datos:** SQL Server, MySQL, MariaDB, MongoDB.
- **Productividad y BI:** Power BI, PowerApps, Power Automate, Excel avanzado.

COMPETENCIAS PERSONALES

- Gestión de incidencias críticas en entornos SOC 24/7 | Documentación técnica de seguridad | Trabajo en equipo multidisciplinar bajo presión | Liderazgo y coordinación técnica | Aprendizaje continuo y adaptación rápida a nuevas herramientas | Atención al detalle
- Carnet de Conducir B y A (España)